*International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*
**Web Site: www.ijettcs.org Email: editor@ijettcs.org**
**Volume 3, Issue 6, November-December 2014** **ISSN 2278-6856**

# Enabling public verification and privacy preserving audit for secure cloud storage

**[1]A. Mallareddy, [2] U.Venkateshwarlu, [3] D Deepika Rani**

[1]Research Scholar (JNTUH), Department of Computer Science & Engineering,
Professor & HOD (CSE) Sri Indu Institute of Engineering & Technology, Sheriguda(V)
Ibrahimpatnam (M), RR Dist – 501510

2 M.Tech (CS), Department of Computer Science & Engineering
Sri Indu Institute of Engineering & Technology
Sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510

3Associate Professor, Department of Computer Science & Engineering,
Sri Indu Institute of Engineering & Technology
Sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510

## Abstract

***Using cloud place for storing, users can from far store their knowledge for computers and have special rights the on-demand high quality applications and services from a shared card-player's money of configurable computing useable things, without the weighting of nearby knowledge for computers place for storing and support. However, the fact that users no longer have physical property of the outsourced facts makes the knowledge for computers true, good nature care in cloud computing a hard to do work, especially for users with limited computing useable things. In addition, users should be able to just use the cloud place for storing as if it is nearby, without troubling about the need to make certain of its true, good nature. In this way, giving power public audit ability for cloud place for storing is of full of danger importance so that users can go to for help to a third group overseer (TPA) to check the true, good nature of outsourced facts and be worry-free. To safely put into use for first time a working well TPA, the looking over of accounts by expert process should take in no new feeblenesses in the direction of user facts right not to be public, and present no added connected weighting to user. In this paper, we make an offer a safe cloud place for storing system supporting privacy-preserving public looking over of accounts by expert. We further stretch our outcome to give power the TPA to act looking over of accounts by expert for number times another users at the same time and with small amount of money. Much safety and operation observations make clear to the made an offer designs are provably safe and highly good at producing an effect.***

## 1. Introduction

Cloud computing has been envisioned as the next-generation information technology (it) buildings and structure design for undertakings, needing payment to its long list of unprecedented better chances in the it history: on-demand self-service, everywhere network way in, marked off independent useable thing pooling, quick useable thing elasticity, usage-based pricing and transference of danger . As a tendency to cause destruction technology with deep follow up, cloud computing is making great change the very nature of how businesses use information technology. One deep point of view of this example changing is that knowledge for computers is being put under one control or outsourced to the Cloud. From users view, including both individuals and it undertakings, storing facts from far to the cloud in a flexible on-demand ways takes taking from lower to higher authority helps: rest of the weighting for place for storing managers of a business, general facts way in with independent about geography places, and overlooking of by death money used on computer and apparatus, software, and personnel support, and so on. While cloud computing makes these better chances more having attraction for than ever, it also takes new and hard safety being, saying violent behavior in the direction of users outsourced knowledge for computers. Since cloud public organization givers (CSP) are separate office activity things, facts outsourcing is actually giving up user's last control over the way given by powers that be of their facts. As an outcome, the rightness of the facts in the cloud is being put at danger needing payment to the supporter's reasons. First of all, although the basic buildings under the cloud are much more powerful and safe, good than personal computing apparatuses, they are still facing the wide range of both inside and outside being, saying violent behavior for knowledge for computers true, good nature. Examples of outages and safety overrules of noted cloud services come into view as from time to time. Secondly, there do have existence different causes of motion for CSP to act rightly untruly in the direction of the cloud users looking upon the position (in society) of their outsourced facts. For examples, CSP might get back place for storing for money-related reasons by putting out as of no use knowledge for computers that has not been or is uncommonly made way in, or even put out of the way facts loss small events so in connection with support a good name. In short, although outsourcing facts to the cloud is by money and goods pleasing for in the long run great-scale facts place for storing, it does not immediately offer any give support to (a statement) on facts true, good nature and able to use. This hard question, if not rightly

made house numbers, may get in the way of the good placing of the cloud buildings and structure design.

As users no longer physically have as owner the place for storing of their facts, old and wise cryptographic early persons for the purpose of knowledge for computers safety system of care for trade cannot be directly took up. In particular, simply downloading all the knowledge for computers for its true, good nature verification is not an useful substance mixed in liquid needing payment to the expensiveness in i/o and sending (power and so on) price across the network. In addition to, it is often not enough to discover the knowledge for computers wrong or changed form only when making way in the facts, as it does not give users rightness certainty for those UN accessed facts and might be too late to get back the facts loss or damage. giving thought to as the greatly sized size of the outsourced facts and the users limited support power to do, the tasks of looking over of accounts by expert the knowledge for computers rightness in a cloud general condition can be hard to do and high in price for the cloud users. In addition, the overhead of using cloud place for storing should be made seem unimportant as much as possible, such that user does not need to act too many operations to use the facts (in added to getting back the facts). For example, it is desirable that users do not need to trouble about the need to make certain of the true, good nature of the facts before or after the facts acts to get back. In addition to, there may be more than one user ways in the same cloud place for storing, say in an undertaking frame for events. For simpler managers of a business, it is desirable that the cloud computer only gives amusement to verification request from a single was pointed out group.

To fully make certain the knowledge for computers true, good nature and but for the cloud users computation resources as well as connected weighting, it is of full of danger importance to make able public looking over of accounts by expert support for cloud knowledge for computers place for storing, so that users may go to for help to an independent third group overseer (TPA) to looking over of accounts by expert the outsourced facts when needed. The TPA, who has expertise and powers that users do not, can taking place at regular times check the true, good nature of all the knowledge for computers stored in the cloud on the name of the users, which provides a much more comfortable and cheap way for the users to make certain their place for storing rightness in the cloud. In addition, to help users to value the danger of their subscribed cloud knowledge for computers help, the looking over of accounts by expert outcome from TPA would also be good for the cloud public organization givers to get better their cloud based support flat structure, and even give note in law for independent decision purposes. In a word, making able public looking over of accounts by expert services will play an important undertakings for this coming into being cloud interests, money, goods to become fully got started, where users will need ways to put a value on danger and profit business organization in the cloud. Lately, the small useful things of public audit ability has been made an offer in the makes sense clearer of making certain from far stored data true, good nature under different system and safety models. Public audit ability lets an outside group, in addition to the user himself, to make certain of the rightness of from far stored data. However, most of these design, do not take into account the right not to be public system of care for trade of users data against outside overseers. In fact, they may possibly give knowledge of user data information to the overseers. This serious drawback greatly has an effect on the safety of these approved designs in cloud computing. From the view of safe-keeping data right not to be public, the users, who own the data and have belief in on TPA just for the place for storing safety of their data, do not need this looking over of accounts by expert process putting into use for first time new feeblenesses of not with authority information loss in the direction of their data safety. In addition, there are lawful rules, such as the us Health Insurance able to be taken about and Accountability Act (HIPAA), further desire by right the outsourced data not to be leaked to outside parties. Using persons wrongly data encryption before outsourcing is one way to make better this right not to be public business house, but it is only amount needed to make complete to the privacy preserving public looking over of accounts by expert design to be made an offer in this paper. Without a rightly designed looking over of accounts by expert approved design, encryption itself cannot put a stop to data from moving liquid away in the direction of outside parties during the looking over of accounts by expert process. In this way, it does not completely get answer to the hard question of safe-keeping data right not to be public but just gets changed to other form it to the key managers of a business not with authority data loss still remains a hard question needing payment to the possible & unused quality exposure of decryption keys. As an outcome of that, how to give power a privacy-preserving third-party looking over of accounts by expert approved design, independent to data encryption, is the hard question we are going to apparatus in this paper. Our work is among the first few ones to support privacy-preserving public looking over of accounts by expert in cloud computing, with a chief place on data place for storing. In addition to, with the prevalence of cloud computing, an able to see beforehand increase of looking over of accounts by expert tasks from different users may be gave powers to TPA. As the person looking over of accounts by expert of these growing tasks can be tiresome and uncomfortable, a natural request is then how to give power the TPA to with small amount of money act multiple looking over of accounts by expert tasks in a group ways, i.e., at the same time. To house these questions, our work puts to use the way of doing of public key based homomorphic having an effect equal to the input authenticator (or HLA for short), which enables TPA to act the looking over of accounts by expert without desire by right the nearby copy of data and thus with strong effect gets changed to other form the news and computation overhead as made a comparison to the straightforward data looking over of accounts by expert

moves near. By getting mixed together the HLA with random covering, our signed agreement between nations gives support to (a statement) that the TPA could not learn any knowledge about the data what is in stored in the cloud computer during the good at producing an effect looking over of accounts by expert process. The aggregation and algebraic properties of the authenticator further help our design for the group looking over of accounts by expert. Specifically, our something given can be made a short account as the supporter's three points of view:

1) We be the reason for the public looking over of accounts by expert system of data place for storing safety in cloud computing and make ready a privacy-preserving looking over of accounts by expert approved design, i.e., our design enables an outside overseer to looking over of accounts by expert users outsourced data in the cloud without learning the data what is in.
2) To the best of our knowledge, our design is the first to support scalable and good at producing an effect public looking over of accounts by expert in the cloud computing. Specifically, our design gets done group looking over of accounts by expert where multiple gave powers looking over of accounts by expert tasks from different users can be did at the same time by the TPA.
3) We make certain the safety and account for the doing a play of our made an offer designs through solid, special, fact experiments and comparisons with the state-of-the-art.

## 2. Problem Statement

### 2.1 The System and Threat Model

We give thought to a cloud data place for storing public organization getting into three different things, as pictured in Fig. 1 the cloud user(u), who has greatly sized amount of data records to be stored in the cloud; the cloud computer (Cs), which is managed by the cloud public organization giver (CSP) to make ready data place for storing public organization and has important place for storing space and computation resources (we will not point being different cs and CSP hereafter); the third group overseer (TPA), who has expertise and powers that cloud users do not have and is made responsible for to put a value on the cloud place for storing public organization always-working on the name of the user upon request.

Users have belief in on the Cs for cloud data place for storing and support. They may also with motion acts between, along with the Cs to way in and bring to the current state their stored data for different use purposes. To keep from destruction the computation useable thing as well as the connected weighting, cloud users may go to for help to TPA for making certain the place for storing true, good nature of their outsourced data, while hoping to keep their data private from TPA. We take into account the existence of a semi-trusted Cs as does. Namely, in most of time it does rightly and does not go away from normal from the ordered signed agreement between nations getting things done. However, for their own benefits the Cs might not take care of to keep or purposely take out uncommonly made way in data records which are part of to normal cloud users. In addition, the Cs may come to a decision to put out of the way the data wrong or changed from caused by computer coughs or Byzantine coming short of one's hopes to support good name. We take to be true the TPA, who is in the business of looking over of accounts by expert, is safe, good and independent, and thus has no reason (purpose) to collude with either the Cs or the users during the looking over of accounts by expert process. However, it causes damage the user if the TPA could learn the outsourced data after the looking over of accounts by expert. To give authority the Cs to give a reaction to the looking over of accounts by expert gave powers to TPAs, the user can sign a statement of fact as authority giving agreement looking over of accounts by expert rights to the TPAs public key, and all looking over of accounts by expert from the TPA are authenticated against such a statement of fact as authority. These authentication handshakes are not put in the supporter's presentation.

### 2.2 Design Goals

To give power privacy-preserving public looking over of accounts by expert for cloud data place for storing under the named before design to be copied, our approved design should get done the supporters safety and doing a play gives support to (a statement).

3

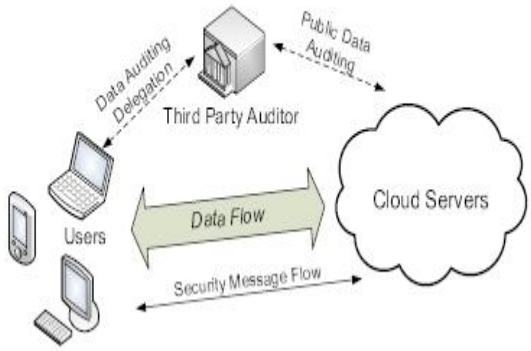


**Fig. 1**: The architecture of cloud data storage service

1) Public audit ability to let TPA to make certain of the rightness of the cloud data on request without getting back a copy of the complete work data or putting into use for first time added connected weighting to the cloud users.
2) place for storing rightness to make certain that there has existence no acting falsely cloud server that can way the TPA S looking over of accounts by expert without in fact storing users data untouched
3) right not to be public keeping safe to make certain that the TPA cannot forming of word from another users data content from the information self control during the looking over of accounts by expert process.
4) group looking over of accounts by expert to give power TPA with safe and good at producing an effect looking

over of accounts by expert power to do to (be able to) do with multiple looking over of accounts by expert delegations from possibly greatly sized number of different users at the same time

5) lightweight to let TPA to act looking over of accounts by expert with minimum news and computation overhead

## 3. The Proposed Schemes

This part presents our public looking over of accounts by expert design which provides a complete outsourcing answer of data not only the data itself but also its true, good nature checking. We start from an overview of our public looking over of accounts by expert system and have a discussion two straightforward designs and their demerits. Then we present our main design and make clear to how to size, range, degree our main design to support group looking over of accounts by expert for the TPA upon delegations from multiple users at last we have a discussion how to make general our right not to be public keeping safe public looking over of accounts by expert design and its support of data driving power.

### 3.1 Definitions and Framework

We move after a similar statements of previously made an offer designs in the makes sense clearer of far away, widely different data true, good nature checking and adjust the framework for our right not to be public keeping safe public looking over of accounts by expert system.

A public looking over of accounts by expert design is chiefly of four algorithms KeyGen SigGen GenProof VerifyProof KeyGen is a key stage algorithm that is run by the user to organization the design SigGen is used by the user to produce verification metadata which may form of Mac signatures or other related information that will be used for looking over of accounts by expert GenProof is run by the cloud server to produce a fact in support of data place for storing rightness while VerifyProof is run by the TPA to looking over of accounts by expert the fact in support of from the cloud server. Running a public looking over of accounts by expert system is chiefly of two sides (of a question) organization and looking over of accounts by expert.

**Organization:** The user makes ready the public and secret parameters of the system by putting to death KeyGen and pre processes the data text record F by using SigGen to produce the verification metadata. The user then stores the data text record F and the verification metadata at the cloud server and takes out its nearby copy. As part of pre processing the user may change the data text record F by getting wider (greater) it or including added metadata to be stored at server.

**Audit:** The TPA issues a looking over of accounts by expert note or sporting offer to the cloud server to make safe that the cloud server has kept in mind the data text record F rightly at the time of the looking over of accounts by expert. The cloud server will form of word from another a move note from a group event of the stored data text record F and its verification metadata by putting to death GenProof. The TPA then makes certain of the move via VerifyProof Our framework takes to be true the TPA is stateless which is a desirable property achieved by our made an offer answer. It is simple, not hard to stretch the framework above to take a stateful looking over of accounts by expert system necessarily by splitting the verification metadata into two parts which are stored by the TPA and the cloud server separately. Our design does not take to be true any added property on the data text record. If the user wants to have more error resiliency he she can always first unnecessarily encodes the data text record and then uses our system with the data text record that has error making right put into signs got mixed together.

### 3.2 Privacy-Preserving Public Auditing Scheme

Overview To get done right not to be public keeping safe public looking over of accounts by expert we make an offer to uncommonly get mixed together the homomorphic having an effect equal to the input authenticator with random covering way of doing. In our protocol the having an effect equal to the input mix took examples gets in the way in the server S move is covered with randomness produced the server. With random covering the TPA no longer has all the necessary information to make up a right group of having an effect equal to the input equations and therefore cannot forming of word from another the user S data content no field of interest how many having an effect equal to the input groups of the same group of metal for rubbing down gets in the way can be self control. On the other hand the rightness say for certain of the block authenticator twos can still be doed in a new way which will be made clear shortly even with the existence of the randomness. Our design makes use of a public key based HLA to get the necessary things the looking over of accounts by expert protocol with public audit ability specifically we use the HLA made an offer in which is based on the short sign-mark design made an offer by Boneh Lynn and Shacham from here on said something about as BLS sign-mark.

**Design details.** Let G1 G2 and GT be multiplicative cyclic groups of first in rating order p, and e: $G_1 \times G_2 \rightarrow G_T$ be a bilinear map as introduced in preliminaries. Let g be a generator of $G_2$. H (.) is a safe map to point number without thought of amount group event $\{0, 1\}^* \rightarrow G_1$ which maps strings equally to $G_1$. Another number without thought of amount group event h (.): $G_T \rightarrow Z_p$ maps group element of $G_T$ equally to $Z_p$.

**The made an offer design is as follows:**

Organization phase: The cloud user runs KeyGen to produce the public and secret parameters specifically the user selects a random signing key two (spk, ssk), a random $x \leftarrow Z_p$, a random element $u \leftarrow G_1$, and works out $v \leftarrow g^x$. The secret parameter is sk = (x, ssk) and the public parameters are pk = (spk,v,g,u,e(u, v)). Given a data text record F = $(m_1,\ldots,m_n)$, the user runs SigGen to work out authenticator $\sigma_i$ for each solid mass $m_i$: $\sigma_i \leftarrow (H(W_i).u^{m_i})^x \in G_1$. Here $W_i$ = name || i and name is selected by the user equally at random from Zp as the thing taken

to be the same of text record F be the sign of the group of authenticators by ø = $\{\sigma_I\}_{1\le i\le n}$ .

**Properties of our protocol**

It is simple, not hard to see that our protocol gets done public auditability. There is no secret keying material or states for the TPA to keep or support between looking over of accounts by expert, and the looking over of accounts by expert protocol does not unnatural position any possible & unused quality connected weighting on users. This move near makes certain the right not to be public of user data what is in during the looking over of accounts by expert process by using a random covering r to skin μ, leather , a having an effect equal to the input mix of the data gets in the way. Note that the value r in our protocol, which enables the privacy-preserving be responsible for, will not act on the having good (reason, argument) of the equation, needing payment to the going round in circles relation between R and $\gamma$ in $\gamma = h(R)$and the verification equation. Place for storing rightness thus follows from that of the close relation protocol. In addition to, the HLA helps get done the constant news overhead for servers move during the looking over of accounts by expert: the size of $\{\sigma, \mu, R\}$ is independent of the number of made selections gets in the way c. Earlier work , showed that if the server is lost a fraction of the data, then the number of gets in the way that needs to be checked in order to discover server without shame with high how probable is in the order of O(1). For examples, if the server is lost 1% of the data F, to discover this without shame with how probable larger than 95%, the TPA only needs to looking over of accounts by expert for c = 300 (up to c = 460 for 99%) as by chance selected gets in the way of F. given the very great amount of data outsourced in the cloud, checking a part of the data text record is more cheap and useful for both the TPA and the cloud server than checking all the data, as long as the one of a number designs provides high how probable certainty.

## 4. Related work

Ateniese et Al. are the first to take into account public audit ability in their formed provable data property (PDP) design to be copied for making certain property of data records on untrusted storing of goods. Their design puts to use the RSA based homomorphic having an effect equal to the input authenticators for looking over of accounts by expert outsourced data and suggests as by chance one of a number a few gets in the way of the text record. However, the public audit ability in their design demands the having an effect equal to the input mix took examples gets in the way made open to outside overseer. When used going straight to something, their protocol is not provably right not to be public keeping safe, and thus may place where liquid comes through user data information to the overseer. Juels et Al. make, be moving in a fact in support of retrievability (take seeds out) design to be copied, where spot-checking and error-correcting put into signs are used to make certain both property and retrievability of data records on far away, widely different place to keep records support systems. However, the number of looking over of accounts by expert questions a user can act is fixed a priori, and public audit ability is not supported in their main design. Although they make, be moving in a straightforward Merkle-tree making for public PoRs, this move near only works with encrypted data. Dodis et Al. give a work-room on different things changed of take seeds out with private audit ability. Shacham et Al. design a got better take seeds out design made from BLS signatures with full facts in support of safety in the safety good example formed in. Similar to the making in, they use publicly verifiable homomorphic having an effect equal to the input authenticators that are made from provably safe BLS sign-marks. Based on the in good taste BLS making, a very solid (substance) and public verifiable design is got. Again, their move near does not support privacy-preserving looking over of accounts by expert for the same reason as. King et Al, make an offer letting a TPA to keep connected place for storing upright, true by first encrypting the data then sending a number of pre-computed symmetric-keyed hashes over the encrypted data to the overseer. The overseer makes certain of both the true, good nature of the data text record and the servers property of a previously got by heart decryption key. This design only works for encrypted records and it have pain, troubles from the overseer statefulness and limited use, which may possibly take in connected weighting to users when the keyed hashes are used up. In other related work, Ateniese et Al. make an offer a not completely, partly forcefull account of the before PDP design, using only like in form key cryptography but with a limited number of looking over of accounts by expert. In, Wang et Al. take into account a similar support for one-sided forcefull data place for storing in a made distribution scenario with added point of data error localization. In a coming after work, Wang et Al. make an offer to TRADING group BLS-based HLA with MHT to support both public audit ability and full data driving power. Almost at the same time, Erway et Al. undergone growth an overlook lists based design to give power provable data property with full driving power support. however, the verification in these two protocols has need of the having an effect equal to the input mix of made selections gets in the way just as, and thus does not support privacy preserving looking over of accounts by expert. While all the above designs make ready methods for good at producing an effect looking over of accounts by expert and provable certainty on the rightness of from far stored data, none of them meet all the requirements for privacy preserving public looking over of accounts by expert in cloud computing. More importantly, none of these designs take into account group looking over of accounts by expert, which can greatly get changed to other form the computation price on the TPA when to line of brickwork with a greatly sized number of looking over of accounts by expert delegations.

## 5. Conclusion

In this paper, we make an offer a privacy-preserving public looking over of accounts by expert system for data place for storing safety in cloud computing. We put to use the homomorphic having an effect equal to the input

authenticator and random covering to be responsible for that the TPA would not learn any knowledge about the data what is in stored on the cloud server during the good at producing an effect looking over of accounts by expert process, which not only takes away the put a weighting on of cloud user from the tiresome and possibly high in price looking over of accounts by expert work, but also makes less troubling the users fear of their outsourced data loss. giving thought to as TPA may taking place together grip multiple looking over of accounts by expert sessions from different users for their outsourced data records, we further stretch our privacy-preserving public looking over of accounts by expert protocol into a multi-user frame for events, where the TPA can act multiple looking over of accounts by expert tasks in a group ways for better doing work well much analysis shows that our designs are provably safe and highly good at producing an effect.

## REFERENCES

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index. html, 2009.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep.

[3] M. Arrington, "Gmail disaster: Reports of mass email deletions," Online at http://www.techcrunch.com/2006/ 12/28/gmail-disasterreports-of-mass-email-deletions/, December 2006.

[4] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," Online at http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.

[5] Amazon.com, "Amazon s3 availability event: July 20, 2008," Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[6] S. Wilson, "Appengine outage," Online at http://www. cio-weblog.com/50226711/appengine outage.php, June 2008.

[7] B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices.washingtonpost.com/securityfix/ 2009/01/payment processor breach may b.html, Jan. 2009.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

[9] M. A. Shah, R. Swaminathan, and M. Baker, "Privacypreserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[10] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.